Gemeente
Hoogezand-Sappemeer

GEMEENTEBLAD

Officiële uitgave van gemeente Hoogezand-Sappemeer.

Nr. 16548
12 februari
2016

Informatiebeveiligingsbeleid

Gemeenten Hoogezand-Sappemeer, Slochteren en Menterwolde

Historie document

Versie	Datum/periode	Opmerkingen
0.1	29 aug 2014	Initieel concept
0.2	02 okt 2014	Verwerking op- en aanmerkingen review door leden werkgroep Informatiebeveiliging als ook vanuit Jos Knijft (unithoofd IUW afdeling Bedrijfsburo, Hoogezand-Sappemeer) en Raymond Hinderks (Automatisering)
0.3	27 okt 2014	Verwerking output review unithoofd IUW afdeling Bedrijfsburo HS.
0.4	11 nov 2014	•Review vanuit Paul Herder (Afdelingshoofd Middelen en Ondersteuning Menterwolde): akkoord, geen verder opmerkingen. •Aanpassingen/aanvullingen termen 'directie' en 'afdelingsmanagers' naar voor alle drie de gemeenten toepasbare organisatorische termen, naar aanleiding van een opmerking van Jessica Siegers (Directeur Bedrijfsvoering Slochteren). Hoogezand-Sappemeer en Menterwolde kennen namelijk 'afdelingen', terwijl Slochteren organisatorisch gezien 'diensten' hanteert. Verder geldt in Menterwolde en Slochteren het gremium 'managementteam' en in Hoogezand-Sappemeer het gremium 'directie'.
1.0	29 jan 2015	Aanpassing diverse datums en ten behoeve van het besluitvormingstraject

Inhoud

1.Managementsamenvatting

De inwoners van onze gemeenten kunnen geen andere overheid kiezen en moeten er daarom op kunnen vertrouwen dat er uiterst zorgvuldig met hun (vertrouwelijke) gegevens wordt omgegaan.

Daarom werken we continue aan de informatieveiligheid binnen onze gemeenten.

Het hieraan ten grondslag liggende beleid wordt middels het treffen van diverse maatregelen vanuit het geldende Informatiebeveiligingsprogramma 2012- 2015 al volop uitgevoerd. Denk bijvoorbeeld aan het goed beveiligen van het uitwisselen van gevoelige, vertrouwelijke informatie via het digitale burgerloket inclusief een audit hierop (Digid) of via Suwi-net en de daaraan verbonden wettelijke (audit)verplichtingen, maar ook aan het realiseren van een ICT-uitwijkomgeving en het succesvol testen ervan.

Met het vaststellen van dit geactualiseerde beleidsdocument 'Informatiebeveiligingsbeleid 1 jan 2015 – 1 jan 2018', geldende voor het samenwerkingsverband tussen de gemeenten Hoogezand-Sappemeer, Slochteren en Menterwolde, zal de basis voor een goede borging van de verdere, integrale doorontwikkeling van onze Informatiebeveiliging, nog steviger worden neergezet. Het betreffende beleid is organisatiebreed en afdeling/dienstoverstijgend, daar waar mogelijk en nodig. Alleen indien strikt nodig, zullen afzonderlijke taakgebied specifieke IB-beleidsmaatregelen gehanteerd worden, zoals een afzonderlijke autorisatieplan voor Suwi of vanuit de Basisregistratie Personen (BRP, voorheen GBA).

Tevens geeft vaststelling van het beleidsstuk, de kaders en richting aan het implementeren van de BIG (Baseline Informatiebeveiliging Nederlandse Gemeenten), als gemeenschappelijk, uniform normenkader voor alle gemeenten) en kunnen we voldoen aan de diverse, hierboven genoemde wettelijke verplichtingen.

Al met al is Informatiebeveiliging namelijk geen vrijblijvendheid meer. Er wordt vanuit het Rijk en de politiek meer en meer ingezet om de gemeente op dit gebied te professionaliseren. Zie de verplichtingen vanuit de in november 2013 door de gemeenten aanvaarde VNG-resolutie, zoals het aansluiten op de IBD (Informatiebeveiligingsdienst), maar ook de diverse informatie-beveiligingsmaatregelen en – audits op het gebied van Suwi, BRP, BAG, Digid en in het kader van de Decentralisaties.

Om dit goed te laten landen, zijn er vanuit het Rijk diverse initiatieven ontplooid, om het onderwerp Informatiebeveiliging hoog op de gemeentelijke agenda te zetten. Denk aan het rechtstreeks aanspreken door de Taskforce BID (Bestuur en Informatieveiligheid Dienstverlening) als van burgemeesters en wethouders op hun verantwoordelijkheden rondom informatiebeveiliging of aan het organiseren voor regionale en landelijke bijeenkomsten voor bestuurders cq gemeentesecretarissen. De Taskforce Bestuur en Informatieveiligheid Dienstverlening is door de Minister van Binnenlandse Zaken en Koninkrijkrelaties (BZK) ingesteld om het onderwerp informatieveiligheid hoog op de agenda te krijgen bij bestuurders en topmanagement van alle overheidslagen. Zowel qua bewustwording als sturing, om de informatieveiligheid van de gegevens van haar inwoners centraal te stellen.

2.Inleiding

Onze gemeentelijke organisatie valt of staat met informatie. Of we nu onze rol als dienstverlener, handhaver, beheerder, control, management/ondersteuning, facilitair, ontwikkelaar of politiek orgaan vervullen, we kunnen niets zonder informatie en informatiesystemen.

Daarom is het van belang dat wij onze informatie beveiligen tegen ongewenste toegang, ongewenste wijziging, ongewenste aantasting en de beschikbaarheid garanderen. Deze informatiebeveiliging bereiken we door het inzetten van een verzameling van beheersmaatregelen, waaronder beleid, werkwijzen,

procedures, organisatiestructuren en programmatuur- en apparatuurfuncties. Onze inwoners vertrouwen erop dat we hun (vertrouwelijke) gegevens afdoende beveiligen.
Het gehele gemeentelijk bestuur (zowel de politieke als ambtelijke bestuurders en leidinggeven) geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitbrengen en handhaven van een informatiebeveiligingsbeleid van en voor de hele gemeente. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.
2.1.Reden voor een actueel Informatiebeveiligingsbeleid
Een aantal landelijke en gemeentelijke ontwikkelingen maken het noodzakelijk, om het Informatiebeveiligingsbeleid te actualiseren en opnieuw vast te stellen:

1. Het uitvoeren van de in november 2013 aanvaarde **VNG Resolutie** '***Informatieveiligheid, als randvoorwaarde voor de professionele gemeente***', inclusief het **aansluiten op de Informatiebeveiligingsdienst** EN het expliciet voldoen aan de '**Baseline voor Informatiebeveiliging Nederlandse Gemeenten' (BIG)**, als gemeenschappelijk, uniform normenkader voor alle gemeenten. Dit normenkader is overigens gebaseerd op de code voor Informatiebeveiliging (vanuit de NEN/ISO 270002 kwaliteitsnormen), waar zowel het 'oude', afzonderlijke Informatiebeveiligingsbeleid van Hoogezand-Sappemeer en Slochteren, als het Informatiebeveiligingsprogramma 2012-2015 al op gebaseerd was;
2. De opkomst van '**moderne' technologieen'**, zoals de doorontwikkeling van de digitale internetdienstverlening en cloudoplossingen, die echter ook tegelijkertijd weer bedreigingen voor de informatieveiligheid met zich meebrengen (de zogenaamde, inmiddels beruchte cybercriminaliteit). Denk tevens aan de toenemende inzet van mobiele devices zoals smartphones en tablets. Zo bieden dergelijke apparaten onze organisatie kansen op het gebied van bereikbaarheid, flexibiliteit en inzet op locatie, maar weten wij op welke wijze adequaat te handelen in geval bjvoorbeeld een Iphone ergens 'vergeten' is of wellicht ontvreemd? Een goede, adequate beveiliging van de mobiele devices en de daarop aanwezige gegevens is van een niet te onderschatten wezenlijk belang.
3. De overheveling van rijkstaken naar de gemeenten: de **3Decentralisaties**. Het gaat het niet alleen meer om de lokale gemeentelijke informatieveiligheid. De mogelijke bedreigingen en risico's strekken verder dan het eigen gemeentelijk grondgebied. Deze schaalvergroting vereist een professionele, integrale aanpak en sturing;
4. Het hebben van een **vastgesteld, actueel Informatiebeveiligingsbeleid is een wettelijke (audit)verplichting,** voortvloeiende vanuit onder andere de wetgeving voor respectievelijk BRP, Digid en Suwi. De nu nog afzonderlijke Informatiebeveiligingsbeleidsdocumenten voor Hoogezand-Sappemeer (beleid geldende voor de periode van februari 2010-februari 2014) en voor Slochteren (beleid geldende voor de periode 2008-2010), zijn verlopen en daarom formeel aan een 'nieuwe' geldigheidsperiode en vaststelling daarvan toe. Voor Menterwolde is geen vastgesteld en geldend Informatiebeveiligingsbeleid voorhanden;
5. De ontstane **samenwerkingsverbanden tussen Hoogezand-Sappemeer, Slochteren en Menterwolde**, ook op het gebied van Informatiebeveiliging en daarbij te komen tot één gezamenlijk, uniform en integraal door te voeren Informatiebeveiligingsbeleid.

2.2. Doel van het document

Dit beleidsdocument legt aan de hand van algemene beleidsuitgangspunten, de geactualiseerde basis voor het taakgebied 'informatiebeveiliging' binnen onze gemeenten en is afgeleid van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
Betreffende Baseline is bedoeld om:

1. Gemeenten op een vergelijkbare manier efficiënt te laten werken met informatiebeveiliging.
2. Gemeenten een hulpmiddel te geven om aan alle eisen op het gebied van informatiebeveiliging

te kunnen voldoen.

3. De auditlast op gemeenten te verminderen.
4. Gemeenten een aantoonbaar betrouwbare partner te laten zijn.

2.3. Uitwerking van het beleid

Dit document dient als kapstok voor verdere inbedding van het informatiebeveiligingsbeleid, de standaarden, de procedures en de processen.
Inbedding zal plaatsvinden door het opstellen en uitvoeren van een gezamenlijk, geactualiseerd Informatiebeveiligingsprogramma (1 januari 2015 – 1 januari 2018) met daarin zowel de al genomen en nog te nemen concrete maatregelen. Deze maatregelen zullen aan de hand van diverse, zo BIG conform mogelijke analyses (risico-, GAP- en impactanalyse) inzichtelijk gemaakt worden.

3. Toelichting IB-Beleid

3.1. Wat is Informatiebeveiliging?

Informatiebeveiliging is de verzamelnaam voor de processen, die ingericht worden om de betrouwbaarheid van gemeentelijke processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen al dan niet opzettelijk onheil. Het begrip 'informatiebeveiliging' heeft betrekking op:

- *beschikbaarheid / continuïteit:* het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- *exclusiviteit / vertrouwelijkheid*: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn;
- *integriteit / betrouwbaarheid:* het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

Door beleid hierop te voeren, biedt het ons bestuur en management sturing op en ondersteuning voor onze informatiebeveiliging.

3.2.Beleidsdeelgebieden

Ons IB-Beleid bevat een aantal deelgebieden, die conform de (strategische variant van de) BIG zijn:

1. Beveiligingsbeleid;
2. Organisatie van informatiebeveiliging;
3. Beheer van bedrijfsmiddelen;
4. Beveiliging van personeel;
5. Fysieke beveiliging en beveiliging van de omgeving;
6. Beheer van communicatie- en bedieningsprocessen;
7. Toegangsbeveiliging;
8. Verwerving, ontwikkeling en onderhoud van informatiesystemen;
9. Beheer van informatiebeveiligingsincidenten;
10. Bedrijfscontinuïteitsbeheer;
11. Naleving.

Ook het IB-programma zal conform deze deelgebieden opgesteld worden.

3.3.Waarom informatiebeveiliging?

Informatie is één van de belangrijkste bedrijfsmiddelen van een gemeente. Toegankelijke en betrouwbare overheidsinformatie is essentieel voor een gemeente, die zich verantwoordelijk gedraagt, aanspreekbaar en servicegericht is, die transparant en proactief verantwoording aflegt aan burgers en raadsleden en die met minimale middelen maximale resultaten behaalt. De bescherming van waardevolle informatie is hetgeen waar het uiteindelijk om gaat. Hoe waardevoller de informatie is, hoe meer maatregelen er getroffen moeten worden.

3.4.Reikwijdte en afbakening informatiebeveiliging

Informatiebeveiliging is meer dan ICT, computers en automatisering. Het gaat om alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, DVD, beeldscherm etcetera) en alle informatie verwerkende systemen (de programmatuur, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen), maar vooral ook mensen en processen. Studies laten zien dat de meeste incidenten niet voortkomen uit gebrekkige techniek, maar vooral door menselijk handelen en een tekort schietende organisatie. Voorbeelden van informatiebeveiligingsmaatregelen zijn: clear desk- en screenbeleid, wachtwoordenbeleid, beveiligingsincidentenbeheer, maatregelen in het kader van de diverse auditverplichtingen (zoals vanuit de wet BRP, BAG, Suwi en Digid), hoe om te gaan met mobiele devices en aanwijzingen voor telewerken.

3.5.Goedkeuring en geldigheid

Dit informatiebeveiligingsbeleid wordt goedgekeurd door ons bestuur en is geldig tot de ingangsdatum van de gemeentelijke herindeling (1 januari 2018). Waarna het opnieuw wordt beoordeeld en indien nodig bijgesteld. Indien nodig zal het informatiebeveiligingsbeleid eerder worden herzien.

3.6. Verantwoordelijkheden en taken informatiebeveiliging

- Ons College is verantwoordelijk voor de vaststelling en wijziging van ons informatiebeveiligingsbeleid en de naleving hiervan.
- De directie (in Hoogezand-Sappemeer)/het managementteam (in Menterwolde en Slochteren) is verantwoordelijk voor de vaststelling en wijziging van ons integrale IB-programma en de uitvoering hiervan.
- Onze managers zijn verantwoordelijk voor de opzet, het bestaan, werking en de naleving van de beveiligingsmaatregelen binnen hun eigen afdeling danwel dienst.
- Onze medewerkers zijn verantwoordelijk voor hun eigen handelen.
- De coördinatie van informatiebeveiliging is belegd bij een daartoe aangewezen functionaris.
- In ons integrale IB-programma worden specifieke verantwoordelijkheden en taken vastgelegd onder deelbeleidsgebied "Organisatie van informatiebeveiliging".

3.7. Randvoorwaarden

- Ons College, de directie (in Hoogezand-Sappemeer)/het managementteam (in Menterwolde en Slochteren) en de managers van cq binnen de diverse afdelingen/diensten dragen het beveiligingsbeleid op passende wijze uit aan alle medewerkers.
- De gemeenteraad (op voorstel vanuit het College) zal, met afweging van de kosten, risico's en baten, voldoende middelen beschikbaar stellen om informatiebeveiliging binnen de gehele organisatie te implementeren en de diverse initiatieven uit het IB-programma uit te laten voeren.
- De directie (in Hoogezand-Sappemeer)/het managementteam (in Menterwolde en Slochteren) en de managers van cq binnen de diverse afdelingen/diensten zullen met de nodige voortvarendheid een herstelactie in gang zetten wanneer naar aanleiding van een beveiligingsincident of audit blijkt dat het beveiligingsniveau onvoldoende is. Dit om te borgen dat de risicoblootstelling adequaat naar een acceptabel niveau terug wordt gebracht.
- Adequate informatiebeveiliging vereist de betrokkenheid en ondersteuning van het gehele personeel (inclusief externe en tijdelijke medewerkers). Daarom worden jaarlijks de verantwoordelijkheden op het gebied van informatiebeveiliging met alle medewerkers besproken. En daar waar nodig worden medewerkers geïnformeerd en zo nodig opgeleid.
- Om onze informatiebeveiliging af te stemmen op interne en externe ontwikkelingen wordt tweejaarlijks een risico-analyse uitgevoerd. Of zodra wijzigingen in de omgeving, technische wijzigingen of dreigingsveranderingen hier aanleiding voor geven.
- Om ervoor te zorgen dat onze informatiebeveiliging "in control" is en blijft, zal informatiebeveiliging worden opgenomen in de planning en control cyclus. Concerncontrol toetst in dat kader of de vastgestelde beveiligingsmaatregelen worden nageleefd.

3.8. Uitgangspunten IB-beleid

Onze gemeenten hanteren bij het opstellen, uitvoeren en managen van het IB-Beleid, de volgende uitgangspunten (ontleend aan de Code voor Informatiebeveiliging (NEN/ISO
27002:2007) en de BIG):
1.Alle informatie en informatiesystemen zijn van kritiek en vitaal belang voor de gemeente. De verantwoordelijkheid voor informatiebeveiliging ligt bij het (lijn)management, met **het College van B&W als eindverantwoordelijke**. De verantwoordelijkheden voor de bescherming van gegevens en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd.
2.Door **periodieke controle, organisatie brede planning én coördinatie** wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het IB-programma (=plan) het fundament onder een betrouwbare informatievoorziening. In het IB-programma wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Het programma wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
3.Informatiebeveiliging is een **continu verbeterproces**. 'Plan, do, check en act' vormen samen het **management systeem** van informatiebeveiliging.
4. De **coördinator informatiebeveiliging** voor de gemeente in de samenwerking, ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover.
5. De gemeente stelt de benodigde **mensen en middelen beschikbaar** om haar eigendommen

en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid.
6.**Regels en verantwoordelijkheden** voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld. Alle medewerkers van de gemeente worden over het gebruik van beveiligingsprocedures geïnformeerd.
7. Iedere medewerker, zowel vast als tijdelijk, intern of extern is **verplicht waar nodig gegevens en informatiesystemen te beschermen** tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.
3.9. Doelgroep

Alle in- en externe medewerkers van de gemeente (inclusief de politieke en ambtelijke bestuurders).
4. Toelichting IB-deelgebieden
4.1. Beveiligingsbeleid

Het belang van informatie(veiligheid)
Informatie is één van de voornaamste bedrijfsmiddelen van <gemeente>. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de bedrijfsvoering maar ook leiden tot imagoschade. Ernstige incidenten hebben mogelijk negatieve gevolgen voor burgers, bedrijven, partners en de eigen organisatie met waarschijnlijk ook politieke consequenties. Informatieveiligheid is daarom van groot belang. Informatiebeveiliging (IB) is het proces dat dit belang dient.

Visie

'De komende jaren zet onze gemeente in op het verhogen van informatieveiligheid en verdere professionalisering van de IB-functie in de organisatie. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van burgers en bedrijven. 1 Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.'

Het proces van informatiebeveiliging is primair gericht op bescherming van gemeentelijke informatie, maar is tegelijkertijd een 'enabler'; het maakt bijvoorbeeld elektronische dienstverlening op verantwoorde wijze mogelijk, evenals nieuwe, innovatieve manieren van werken. De focus is informatie uitwisselen in alle verschijningsvormen, zoals elektronisch, op papier en mondeling. Het gaat niet alleen over bescherming van privacy, maar ook over bescherming van vitale maatschappelijke functies die worden ondersteund met informatie (verkeer, vervoer, openbare orde en veiligheid, etc.). Het gaat ook niet alleen over ICT: verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid.

Doelstelling

Dit informatiebeveiligingsbeleid (IB-beleid) is het kader voor passende technische en organisatorische maatregelen om gemeentelijke informatie te beschermen en te waarborgen, dat de gemeente voldoet aan relevante wet en regelgeving. We streven er naar om 'in control' te zijn en daarover op professionele wijze verantwoording af te leggen. In control betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn en dat er een SMART-planning is
van de maatregelen die nog niet genomen zijn en als laatste dat dit geheel verankerd is in de PDCA-cyclus.

Uitgangspunten

- Het informatiebeveiligingsbeleid van onze gemeente is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.
- Het beleid is gebaseerd op de Code voor Informatiebeveiliging (NEN/ISO 27002) en de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
- Het IB-beleid wordt vastgesteld door het college van B&W. De directie (in Hoogezand-Sappemeer)/het managementteam (in Menterwolde en Slochteren) herijkt periodiek het IB-programma aan maatregelen.
- Het uitvoeren van de in november 2013 door de gemeenten aanvaarde VNG resolutie 'informatieveiligheid'. Van deze resolutie zijn de belangrijkste punten:
  1. Informatieveiligheid wordt onderdeel van de collegeambities 2014-2018 en wordt opgenomen in de portefeuille van één van de leden van het college van B&W;
  2. Gemeenten zorgen voor verankering van informatieveiligheid op de gemeentelijke agenda, waarbij het college de gemeenteraad informeert;
  3. Bestuurlijke en organisatorische borging van informatieveiligheid, door aansluiting in de planning- en controlcyclus;
  4. Toetsing door een interbestuurlijke visitatiecommissie of de resolutie in voldoende mate wordt uitgevoerd;
  5. Gemeenten stellen de Baseline Informatiebeveiliging Gemeenten vast als het gemeentelijk basisnormenkader voor informatieveiligheid;
  6. De gemeenten maken de lokale invulling rondom het thema van informatieveiligheid transparant voor burgers, bedrijven en (keten)partners;
  7. Het aansluiten op de Informatiebeveiligingsdienst, waardoor de gemeente gerichte waarschuwingen over mogelijke digitale kwetsbaarheden en dreigingen (cybercrime) kan ontvangen om vervolgens sneller en adequaat de nodige tegenmaatregelen te kunnen treffen.

Het aansluiten op de IBD bestaat uit de volgende
stappen:

1. Benoemen ACIB (algemeen contactpersoon InformatieBeveilliging)
1. Formeel benoemen VCIB (vertrouwelijk contactpersoon InformatieBeveiliging
2. Aanleveren gemeentelijke IP-adressen en URLS
3. Aanleveren gemeentelijke ICT-foto (CMDB van binnen de gemeente

gebruikte hard- en sofftware)
Hiertoe hebben we inmiddels stappen 1 en 2 succesvol uitgevoerd. Door het
formeel benoemen van een Coördinator Informatiebeveiliging en deze functionaris tevens aan te wijzen als VCIB richting IBD.

Risico, indien niet op orde

Het College, de directie (in Hoogezand-Sappemeer)/het managementteam (in Menterwolde en Slochteren) kunnen niet sturen op en ondersteuning bieden aan IB-beveiliging overeenkomstig de bedrijfsmatige - en wettelijke verplichtingen. Voorbeeld, BRP-wetgeving (voorheen GBA), Digid-audit, Suwi-audit en vanuit de VNG resolutie, wordt een vastgesteld IB-beleid vereist.

Indien we geen vastgesteld, actueel IB-beleid hebben, voldoen we niet aan onze wettelijke verplichtingen en bestaat het risico dat de gemeente hierop aangesproken wordt en dat er afsluiting van een landelijke koppeling (zoals Digid of Suwi) dreigt.
4.2.Organisatie van de informatiebeveiliging
Doelstelling
Beheren van de informatiebeveiliging (IB) binnen de organisatie.
Er is een beheerkader vastgesteld om de implementatie van informatiebeveiliging in de organisatie te initiëren en te beheersen.
Goedkeuring door de directie (in Hoogezand-Sappemeer)/het managementteam (in Menterwolde en Slochteren) van het informatiebeveiligingsbeleid, de toewijzing van de rollen en de coördinatie en beoordeling van de implementatie van het beleid binnen de organisatie.
Risico, indien niet op orde
Zonder beheerorganisatie kun je geen invulling geven aan je informatiebeveiligingsbeleid.
Vanuit onder andere BRP-wetgeving, Digid-audit, Suwi-audit en vanuit de VNG resolutie, wordt een aantoonbare organisatie van de informatiebeveiliging vereist.
Indien we hiertoe geen beheersorganisatie hebben, voldoen we niet aan onze wettelijke verplichtingen en bestaat het risico dat de gemeente hierop aangesproken wordt en leidt het mogelijk tot afsluiting van een landelijke voorziening (zoals Digid of Suwi).
Met ingang van 28 september 2012 is er een beveiligingsorganisatie neergezet. Onder verantwoordelijkheid van de directie (in Hoogezand-Sappemeer)/het managementteam (in Menterwolde en Slochteren) zijn de werkgroepleden Informatiebeveiliging HS-SL verantwoordelijk voor de implementatie van de maatregelen. In deze werkgroep zijn vertegenwoordigers vanuit Personeelsbeleid, Automatisering, Gebouwenbeheer, Informatiemanagement, BRP, Rijbewijzen en Reisdocumenten, Suwi (op ad-hoc basis) vertegenwoordigd. Betreffende werkgroep wordt voorgezeten door de Coördinator Informatiebeveiliging.
4.3.Beheer van bedrijfsmiddelen
Doelstelling
Het handhaven van een adequate bescherming van bedrijfsmiddelen (NB gaat om ALLE bedrijfsmiddelen.
Risico, indien niet op orde
- Bedrijfsmiddelen en informatie zijn blootgesteld aan risico's zoals diefstal, beschadiging of onoordeelkundig gebruik, waarbij niet voor alle ICT-configuratie items is vastgelegd wie de eigenaar/hoofdgebruiker is.
- Wanneer de bedrijfsmiddelen niet zijn toegewezen aan een eigenaar bestaat het risico dat ook niemand verantwoordelijkheid neemt voor de benodigde beveiligingsmaatregelen.
  4.4. Beveiliging van personeel

Doelstelling
- Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen.
- De verantwoordelijkheden ten aanzien van beveiliging is vóór het dienstverband vastgelegd in passende functiebeschrijvingen en in de arbeidsvoorwaarden.
- Alle kandidaten voor een aanstelling, ingehuurd personeel en externe gebruikers worden gescreend, in het bijzonder voor vertrouwensfuncties.
- Werknemers, ingehuurd personeel en externe gebruikers, die ICT-voorzieningen gebruiken tekenen een overeenkomst over hun beveiligingsrollen en –verantwoordelijkheden.

Risico, indien niet op orde
Het aannemen of inhuren van nieuw personeel en het laten verrichten van werkzaamheden door externe medewerkers verdient extra aandacht, omdat menselijk falen en bedreigingen van menselijke aard significante invloed kunnen hebben op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie.
4.5.Fysieke beveiliging en beveiliging van de omgeving
Doelstelling
- Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie, bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten.
- ICT-voorzieningen,die kritieke of gevoelige bedrijfsactiviteiten ondersteunen, behoren fysiek te worden ondergebracht in beveiligde ruimten, beschermd door afgegrensde beveiligde gebieden, in een gecontroleerde omgeving, beveiligd met geschikte beveiligingsbarrières en toegangsbeveiliging. Ze behoren fysiek te worden beschermd tegen toegang door onbevoegden, schade en storingen.
- Het voorkomen van verlies, schade of diefstal van apparatuur en bescherming tegen fysieke bedreigingen en gevaren van buitenaf.

Risico, indien niet op orde

- Onbevoegde toegang tot kritieke systemen of waardevolle informatie. Bij het ontbreken van registratie zijn incidenten bovendien niet herleidbaar tot individuen.
- Door bijvoorbeeld de inzet van externen, de toeloop van leveranciers en andere niet-medewerkers of het feit dat de medewerkers op meerdere locaties op geruime afstand van elkaar gevestigd zijn, is het betrekkelijk eenvoudig voor niet-medewerkers om toegang tot de panden te krijgen door tegelijk met een geautoriseerde medewerker naar binnen te gaan.
- Als informatie zichtbaar op bureaus ligt, is er een verhoogd risico m.b.t. de vertrouwelijkheid.
- Geen procedures voor het veilig verwijderen of hergebruiken van ICT-apparatuur.
- Bescherming van apparatuur, waaronder apparatuur die buiten de locatie wordt gebruikt en het verwijderen van bedrijfseigendommen, is noodzakelijk om het risico van toegang door onbevoegden tot informatie te verminderen en om de apparatuur en informatie te beschermen tegen verlies of schade.

4.6. Beheer van communicatie- en bedieningsprocessen

(Beveiliging van apparatuur en informatie)
Doelstelling
- Waarborgen van een correcte en veilige bediening van ICT-voorzieningen.
- Vastgestelde verantwoordelijkheden en procedures voor beheer en bediening van alle ICT-voorzieningen. Dit omvat tevens de ontwikkeling van geschikte bedieningsinstructies.
- Toepassing, waar nodig, van functiescheiding om het risico van nalatigheid of opzettelijk misbruik te verminderen.

Risico, indien niet op orde
- Het ontbreken van documentatie kan leiden tot fouten, niet-uniforme wijze van gegevensinvoer, of in geval de beheerder/bediener uitvalt, tot problemen rondom de continuïteit.
- Onjuiste autorisaties kunnen leiden tot foutieve handelingen, fraude en verduistering.
- Het niet uitvoeren en vastleggen van technische en functionele applicatietesten en/of de resultaten hiervan, kan in bepaalde omstandigheden (tijdsdruk, vakantieperiodes, etc.) leiden tot een verhoogd risico van uitval of gegevens verlies.
- De gemeente gaat steeds meer samenwerken (en informatie uitwisselen) in ketens en besteedt meer taken uit. Bij beheer van systemen en gegevens door een derde partij, kan ook informatie van de gemeente op straat komen te liggen. De gemeente blijft verantwoordelijk voor de informatiebeveiliging van haar gegevens in dat deel van de keten, waarbij het beheer bij een andere partij ligt.
- Programmatuur en ICT-voorzieningen zijn kwetsbaar voor virussen.
- Het ontbreken van een regeling voor antivirus bescherming bij medewerkers thuis leidt tot hogere beveiligingsrisico's.

4.7. (Logische) Toegangsbeveiliging

Doelstelling
Voorkomen onbevoegde toegang tot het centrale ICT-domein van de organisatie
Risico, indien niet op orde
- Wanneer toegangsbeheersing niet expliciet gebaseerd is op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en/of een aanvullende risicoanalyse, is niet duidelijk of het juiste niveau van beveiliging wordt gehanteerd.
- Verstoringen door onjuist cq niet geauthoriseerd gebruik van ICT-ruimtes of ICT-componenten (m.n. waar ook niet ICT-teams toegang hebben).

De identiteit van een gebruiker die toegang krijgt tot gemeentelijke informatie dient te worden vastgesteld. Logische toegang is gebaseerd op de classificatie van de informatie.
4.8.Verwerving, ontwikkeling en onderhoud van informatiesystemen
Doelstelling
Beveiliging bij ontwikkel en ondersteuningsprocessen.
Risico, indien niet op orde
- Verstoring in de continuiteit en beschikbaarheid van de informatiesystemen.
- Incorrecte verwerking, verlies, onbevoegde modificatie en ongeauthoriseerd gebruik van informatie

4.9. Beheer van informatiebeveiligingsincidenten

Doelstelling
- Bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden, die verband houden
- met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.

- Formele procedures voor rapportage van gebeurtenissen en escalatie. Alle werknemers, ingehuurd personeel en externe gebruikers zijn op de hoogte van deze procedures voor het rapporteren van de verschillende soorten gebeurtenissen en zwakke plekken die invloed kunnen hebben op de beveiliging van de bedrijfsmiddelen.
- Er is een verplichte meldingssystematiek in werking om alle informatiebeveiligingsgebeurtenissen en zwakke plekken zo snel mogelijk te rapporteren aan de aangewezen contactpersoon.

Risico, indien niet op orde
Als incidenten niet geregistreerd worden, is niet duidelijk waar en wanneer er zich incidenten voor doen of voor hebben gedaan. Op deze wijze kan er geen lering worden getrokken uit deze incidenten om deze in de toekomst te voorkomen of om preventief betere maatregelen te implementeren.
4.10.Bedrijfscontinuïteitsbeheer
Doelstelling
- *Onderbreken van bedrijfsactiviteiten tegengaan en kritische bedrijfsprocessen beschermen*
- *tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.*
- *Een adequaat beheerproces van bedrijfscontinuïteit om de uitwerking op de organisatie, veroorzaakt door het verlies van informatie en het herstellen daarvan tot een aanvaardbaar niveau te beperken.*
- *Informatiebeveiliging is een integraal onderdeel van het totale bedrijfscontinuïteitsproces en andere beheerprocessen binnen de organisatie.*

Risico, indien niet op orde
Onderbreking van bedrijfsactiviteiten en kritische bedrijfsprocessen als gevolg van omvangrijke storingen in informatiesystemen of rampen
4.11.Naleving
Doelstelling
- Voorkomen schending wet- en regelgeving of contractuele verplichtingen.
- Beoordeling naleving van het beveiligingsbeleid.
- Richtlijnen bij audits informatie systemen

Risico, indien niet op orde
De kans op genoemde risico's vanuit de IB-deelgebieden neemt toe als er niet wordt nageleefd.
Dit IB-beleid treedt in werking na vaststelling door college van B&W. Hiermee komt het oude IB-beleid van de gemeente Hoogezand-Sappemeer van 2010 en het oude IB-beleid van de gemeente Slochteren van 2008 te vervallen.
Aldus vastgesteld door:
Burgemeester en wethouders van *gemeente Hoogezand-Sappemeer*op ……………………………….. 2015,
[Naam. Functie] [Naam. Functie]
Burgemeester en wethouders van *gemeente Slochteren*op …………………………………………………. 2015,
[Naam. Functie] [Naam. Functie]
Burgemeester en wethouders van *gemeente Menterwolde*op ……………………………………………….. 2015,
[Naam. Functie] [Naam. Functie]